**SUPREMA ACCESS CONTROL AND TIME ATTENDANCE PLATFORM - BioStar 2**

**TECHNICAL SPECIFICATIONS**

2023-07-31

# ABBREBIATIONS

**AC** Access Control

**AES** Advanced Encryption Standard

**AoC** Access-on-Card

**APB** Anti-passback

**Auth** Authentication

**DB** Database

**DHCP** Dynamic Host Configuration Protocol

**HTTPS** Hypertext Transfer Protocol over Secure Socket

**PIN** Personal Identification Number

**SHA** Secure Hash Algorithm

**TA** Time Attendance

**VE** Video Event

# PART 1 - GENERAL

This document intent is to specify the minimum criteria for the design, supply, installation, and commissioning of the BioStar 2 which is a web-based security platform.

* 1. SUMMARY

1. Section includes a web-based security platform requirements
2. Product - A web-based security platform, capable of managing access control system, managing time attendance system, recording video log with Ethernet network connectivity, and managing visitor system.
   1. SUBMITTALS
   2. QUALIFICATIONS
3. All installation, configuration, and setup of the platform shall provide by qualified technicians.
4. Installers shall be trained by the Manufacturer to install, configure and commission the access control and time attendance system.

END OF SECTION

# PART 2 - PRODUCTS

1. MANUFACTURER
2. Suprema Inc.   
   17F Parkview Office Tower, Jeongja, Bundang, Seongnam, Gyeonggi, 463-863, Republic of Korea  
   Tel: 82-31-783-4502, Fax: 82-31-783-4503, [www.supremainc.com](http://www.supremainc.com)  
   <http://support.supremainc.com>
3. This specification is based on BioStar 2.8.12 manufactured by Suprema Inc.
4. MINIMUM SYSTEM REQUIREMENT
5. Access Control and Time Attendance
6. Small Business Server
7. Total devices: 50
8. Computer
9. 2 GHz Dual Core CPU
10. 8 GB RAM
11. 512 GB SSD
12. Operating system
13. Windows 7 (SP1 or later)
14. Windows 8
15. Windows 8.1
16. Windows 10
17. Windows 11
18. Windows Server 2008 R2 (SP2 or later)
19. Windows Server 2012
20. Windows Server 2012 R2
21. Windows Server 2016
22. Windows Server 2019
23. Windows Server 2022

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome 75 or later
9. Medium Business Server
10. Total devices: 100
11. Computer
12. 4 GHz Quad-core CPU
13. 16 GB RAM
14. 1 TB SSD
15. Operating system
16. Windows 7 (SP1 or later)
17. Windows 8
18. Windows 8.1
19. Windows 10
20. Windows 11
21. Windows Server 2008 R2 (SP2 or later)
22. Windows Server 2012
23. Windows Server 2012 R2
24. Windows Server 2016
25. Windows Server 2019
26. Windows Server 2022

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome 75 or later
9. Enterprise Business Server
10. Total devices: 1,000
11. Computer
12. 4 GHz 16 Core CPU
13. 32 GB RAM
14. 1 TB SSD
15. Operating system
16. Windows 7 (SP1 or later)
17. Windows 8
18. Windows 8.1
19. Windows 10
20. Windows 11
21. Windows Server 2008 R2 (SP2 or later)
22. Windows Server 2012
23. Windows Server 2012 R2
24. Windows Server 2016
25. Windows Server 2019
26. Windows Server 2022

▪ Windows virtual environments on Mac Boot Camp are not supported.

1. Database
2. MariaDB 10.1.10
3. MS SQL Server 2012
4. MS SQL Server 2014 SP2
5. MS SQL Server 2016 SP1
6. MS SQL Server 2017
7. MS SQL Server 2019
8. Client Web Browser: Google Chrome 75 or later
9. Video Log
10. Computer (Minimum)
11. 4 GHz Quad-core CPU
12. 8 GB RAM
13. 2 TB HDD
14. Computer (Recommended)
15. 4 GHz Quad-core CPU
16. 16 GB RAM
17. 4TB HDD
18. BioStar 2 API Server
19. Computer (Minimum)
20. 4 GHz Quad-core CPU
21. 8 GB RAM
22. 1TB Free disk space
23. Computer (Recommended)
24. 4 GHz Quad-core CPU
25. 16 GB RAM
26. 2 TB Free disk space
27. PERFORMANCE CRITERIA
28. System Architecture
29. A web-based security platform, capable of managing access control system, managing time attendance system, recording video log with Ethernet network connectivity, and managing visitor system.
30. Access Control
31. User management
32. Device management
33. Door management
34. Elevator management
35. Zone management (Anti-passback, Fire Alarm, Schedule Lock, Schedule Unlock, Intrusion Alarm, Interlock, Muster, Occupancy Limit)
36. Access group management
37. Monitoring (Event log, Real-time log, Device status, Door status, Floor status, Zone status, Image log, Alert history and Graphic Map)
38. Alarm management
39. RFID card management
40. Audit trail
41. Report
42. Time Attendance
43. Time code management
44. Shift management
45. Schedule template management
46. Overtime rule management
47. Schedule management
48. Leave management
49. Monitoring (Leave and Exception)
50. TA report generation
51. Video Log
52. Visitor Management
53. Standard Transmission Control Protocol (TCP/IP) networking communication protocol between servers, clients, and devices.
54. Support Dynamic Host Configuration Protocol (DHCP) or Static IP address.
55. Support network configuration.
56. Support Network Time Protocol (NTP).
57. Support HTTPS communication protected by Secure Socket Layer (SSL) between the client (Web browser) and platform.
58. Support AES-256 for User Name, Fingerprint Template, and Face Template.
59. Support AES-256 for Fingerprint Template and Face Template (Optional).
60. Support SHA-256 for PIN and Password.
61. Support export to CSV or PDF for list items.
62. Installation Wizard
63. Separate standalone installation package.
64. Shall support English and Korean.
65. Shall allow a user to perform the initial configuration.
66. Shall set the password for the admin account.
67. Shall select the database installation (MariaDB 10.1.10 or Custom).
68. Shall set the root password for MariaDB.
69. Shall set the custom database information including Server IP, Server Port, AC DB name, AC DB login information, TA DB login information, TA DB name, VE DB login information, and VE DB name.
70. Shall check the database connection.
71. Shall generate the database tables.
72. Shall change the port number for server.
73. Shall install the USB Device Agent for BioMini and DUALi DE-620.
74. License and System Capacity
75. License for Access Control

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Items** | | **Starter (Free)** | **Basic** | **Standard** | **Advanced** | **Professional** | **Enterprise** |
| **Access Control** | Max. User | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited | Unlimited |
| Max. Device | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 | 1,000 |
| Max. Door | 5 | 20 | 50 | 100 | 300 | 1,000 |
| Zone | - | - | Supported | Supported | Supported | Supported |
| Elevator | - | - | - | Supported | Supported | Supported |
| Graphic Map | - | - | - | Supported | Supported | Supported |
| Server Matching | - | - | - | Supported | Supported | Supported |
| Cloud | - | - | Supported | Supported | Supported | Supported |
| Active Directory | - | - | - | Supported | Supported | Supported |

2. License for Time Attendance

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Items** | **Starter (Free)** | **Standard** | **Advanced** | **Professional** |
| **Number of Users** | 100 | 500 | 1,000 | Unlimited |

3. License for Video

|  |  |  |
| --- | --- | --- |
| **Items** | **Starter (Free)** | **Video License** |
| **Video Log** | - | Supported |

4. License for Visitor

|  |  |  |
| --- | --- | --- |
| **Items** | **Starter (Free)** | **Visitor License** |
| **Visitor Management** | - | Supported |

1. Interface
2. Use a Web-based client user interface for configuration, administration, management, and monitoring.
3. Support for multi-lingual UI
4. English and Korean available.
5. Other languages available via language pack from website. (Supported languages may vary depending on the BioStar 2’s version)
6. German (Deutsch)
7. Latin Spanish
8. Spain Spanish
9. French
10. Italian
11. Japanese
12. Dutch (Nederlands)
13. Portuguese
14. Chinese
15. Russian
16. Arabic
17. Romanian
18. User
19. User ID
20. Support numeric user ID.
21. Support alphanumeric user ID (Optional).
22. Supports expiration dates (Period) for the user.
23. Supports card printing for user.
24. Operator levels
25. Provide for a maximum of 6 pre-defined levels.
26. Provide for an unlimited number of custom operator levels.
27. Each level shall have a set of permissions and shall be able to be configured for different operator levels.
28. Custom Field
29. Provide 3 types of custom user fields.
30. Support the Text Input Box, Number Input Box, and Combo Box
31. Provide for a maximum of 20 custom fields.
32. Fingerprint
33. Support up to 10 fingers (20 templates) per user.
34. Support 3 types of fingerprint template format (SUPREMA / ISO 19794-2 / ANSI 378).
35. Face
36. Support up to 5 faces (150 templates) per user.
37. Visual Face
38. Support up to 2 faces per user and 20 templates (40 templates) per face.
39. Support Visual Face Mobile Enrollment.
40. Wiegand Card
41. Provide for a maximum of 15 customized formats including 5 pre-defined formats.
42. Support card formats with total bits, facility code, customizable ID fields, and parity bits.
43. Provide for a maximum of 5 pre-defined formats.
44. 26 bit SIA Standard-H10301
45. HID 37 bit-H10302
46. HID 37 bit-H10304
47. HID Corporate 1000
48. HID Corporate 1000 48bit
49. Smart Card
50. Support 3 types of smart card layout and mobile card.
51. MIFARE, iCLASS, DESFire, iCLASS Seos and Mobile
52. Store the fingerprint templates on the smart card up to 4. (Access-on Card)
53. Mobile Access
54. Support the connection with the Suprema Mobile Portal.
55. Issue and revoke mobile access cards remotely.
56. QR/Barcode
57. Support 2 types of QR/Barcode.
58. BioStar 2 QR: Directly issue a QR code that contains an encrypted PIN and card ID on BioStar 2.
59. QR/Barcode: Register users with QR/Barcodes issued from 3rd-party systems.
60. Import/Export User Information via CSV file
61. Support import and export data in Comma-separated Values (CSV) file format.
62. Support multiple languages.
63. Allow the user to import/export the user information and card information in CSV file.
64. Support the auto/manual mapping of CSV fields to the database fields.
65. Support long-term idle user management.
66. Device
67. Support auto search and manual search for a device.
68. Allow the user to change the device settings and perform the action that includes:
69. Firmware upgrade
70. Factory reset
71. Lock/Unlock
72. Time zone
73. Time synchronization
74. Network configuration
75. Serial (RS-485) configuration
76. Authentication settings
77. Card format settings
78. Trigger & action
79. Time attendance settings
80. Administrator level
81. Display and sound settings
82. Wiegand settings
83. Auto synchronization with server
84. Thermal camera and mask settings
85. Door
86. Supported door configuration includes:
87. Two devices (entry device and exit device) for one door
88. Entry device for one door with exit button
89. Entry device for one door without exit button
90. Support two types of relay setting for the exit button and door sensor.
91. Normally open and normally closed
92. Allow the user to configure the door settings that include:
93. Entry device selection
94. Relay selection for a door lock
95. TTL input port for an exit button
96. TTL input port for a door sensor
97. Relay release time for door lock
98. Dual authentication settings
99. Held open time and alarm
100. Forced open alarm
101. Anti-passback alarm
102. Elevator
103. Support the floor button control.
104. Support auto/manual mapping of floor names to the relay numbers.
105. Allow the user to configure the floor control that includes:
106. Controller selection
107. Reader selection
108. Module selection
109. Total number of floors
110. Relay release time for the floor button
111. Dual authentication settings
112. Tamper port setup
113. Alarm configuration
114. Trigger & Action
115. Zone
116. Anti-passback
117. User shall be able to define the areas and assign the entry devices and exit devices to configure an anti-passback zone.
118. Support the global APB zone which can be set with all devices enrolled in BioStar 2.
119. Support the local APB zone which can be set with the entry devices and exit device connected with RS-485.
120. Allow the user to configure an anti-passback zone that includes:
121. APB zone mode (Global or Local)
122. Temporary activation or deactivation of the APB zone
123. APB type (Hard APB or Soft APB)
124. Auto reset time
125. Entry device and exit devices selection for the APB zone
126. Network failure action
127. Customizable signal output for alarm
128. Bypass user group configuration
129. Fire Alarm
130. User shall be able to define the areas and assign the doors and/or elevators to configure a fire alarm zone.
131. Support the global fire alarm zone which can be set with all devices enrolled in BioStar 2.
132. Support the local fire alarm zone which can be set with the entry devices and exit device connected with RS-485.
133. Allow the user to configure a fire alarm zone that includes:
134. Fire alarm zone mode (Global or Local)
135. Temporary activation or deactivation of the Fire Alarm zone
136. Door and/or elevator selection for the fire alarm zone
137. Customizable signal output for alarm
138. Scheduled Lock
139. User shall be able to define the areas and assign the doors and schedule to configure a scheduled lock zone.
140. Allow the user to configure a scheduled lock zone that includes:
141. Temporary activation or deactivation of the Scheduled Lock zone
142. Door lock method selection
143. Door and schedule selection for the scheduled lock zone
144. Customizable signal output for alarm
145. Bypass user group configuration
146. Scheduled Unlock
147. User shall be able to define the areas and assign the doors and schedule to configure a scheduled unlock zone.
148. Allow the user to configure a scheduled unlock zone that includes:
149. Temporary activation or deactivation of the Scheduled Unlock zone
150. Started by user authentication option
151. Door and schedule selection for the scheduled unlock zone
152. Access group where the user belongs who can start a scheduled unlock
153. Intrusion Alarm
154. User shall be able to define the areas and assign the doors to configure an intrusion alarm zone.
155. Support the global intrusion alarm zone which can be set with all devices enrolled in BioStar 2.
156. Support the local intrusion alarm zone which can be set with the entry devices and exit device connected with RS-485.
157. Allow the user to configure an intrusion alarm zone that includes:
158. Intrusion alarm zone mode (Global or Local)
159. Temporary activation or deactivation of the Intrusion Alarm zone
160. Door selection for detecting intrusion
161. Arm and/or disarm settings
162. Customizable signal output for detecting intrusion alarm
163. Customizable signal output when a specified event occurs
164. Interlock
165. User shall be able to define the areas and assign the doors to configure an interlock zone.
166. Support the local interlock zone which can be set with the devices connected to CoreStation with RS-485.
167. Allow the user to configure an interlock zone that includes:
168. Temporary activation or deactivation of the Interlock zone
169. Door selection for the interlock zone
170. Option to detect the user's stay in the interlock zone
171. Customizable signal output for alarm
172. Muster
173. User shall be able to define the areas and assign the entry & exit devices and the access group to configure a muster zone.
174. Support the global muster zone which can be set with all devices enrolled in BioStar 2.
175. Allow the user to configure a muster zone that includes:
176. Temporary activation or deactivation of the Muster zone
177. Door and access group selection for the muster zone
178. Maximum amount of time that user can stay in the muster zone
179. Customizable signal output for alarm
180. Occupancy Limit
181. Users shall be able to define the areas and assign the entry & exit devices and limit the count to configure an occupancy limit zone.
182. Support the global occupancy limit zone, which can be with FaceStation F2 and FaceStation 2 added on BioStar 2.
183. Allow the user to configure an occupancy limit zone that includes:
184. Temporary activation or deactivation of the occupancy limit zone
185. Entry and exit devices selection for the occupancy limit zone
186. The maximum number of people who can enter the Occupancy limit zone
187. Access Control
188. Provide the access permission status by four pre-defined filters.
189. Door permission by Access Group
190. Elevator permission by Floor Level
191. Access Level
192. Support the user to create an access level which is combined with the doors and schedules.
193. Floor Level
194. Support the user to create a floor level which is combined with the elevators, floor names, and schedules.
195. Access Group
196. Support the user to create an access group for door access permission which is combined with the access levels and user groups/individual users.
197. Support the user to create an access group for floor access permission which is combined with the floor levels and user groups/individual users.
198. Monitoring
199. Provide export the access control event list to the CSV file.
200. Support the filter functionality for sort.
201. Provide all monitoring features of the access control system that includes:
202. Event log
203. Real-time log
204. Device Status
205. Door Status
206. Floor Status
207. Zone Status
208. Alert History
209. Graphic Map View
210. Provide the following operations for the selected door in Door Status.
211. Lock the door manually
212. Unlock the door manually
213. Release the manual lock/unlock
214. Open the door temporarily
215. Clear all door alarm
216. Clear the APB alarm
217. Provide the following operations for the selected floor in Floor Status.
218. Lock the floor manually
219. Unlock the floor manually
220. Release the manual lock/unlock
221. Open the floor temporarily
222. Clear all floor alarm
223. Provide the following operations for the selected zone in Zone Status.
224. Clear the APB alarm
225. Clear all alarm
226. Video
227. Record the video when occurs the specified access control event at door.
228. Support the user to change the video file path.
229. Support the user to change the weeks to keep the recorded files.
230. Support NVR setup and IP camera setup.
231. Support NVR manufacturers including:
232. ACTi
233. Dahua
234. Hikvision
235. Time Attendance
236. Support the user to configure a time attendance rule and tracking the TA records including:
237. Time code
238. Shift
239. Schedule Template
240. Rule
241. Schedule
242. TA Report
243. TA report shall include 8 pre-defined reports type that can be customized by the user:
244. Daily
245. Daily Summery
246. Individual
247. Individual Summery
248. Leave
249. Exception
250. Edit History
251. Working alarm time
252. Support the filter functionality for customized TA report.
253. Support the user to export the TA reports as CSV or PDF files.
254. Support the user to modify the TA records.
255. Visitor
256. Provide the visit application page for visitors:
257. Support the terms and conditions and the privacy policy information for visitors.
258. Support the fingerprint enrollment and card issuance for visitors.
259. Support to the USB fingerprint scanner connection.
260. BioMini
261. BioMini Plus
262. BioMini Plus 2
263. Support the shortcut of the visitor application page.
264. Provide the visitor management menu:
265. Support the list of registered, checked in, checked out, and total visitors.
266. Support the visitor search.
267. Support access control for visitors.
268. System Alert
269. Provide the user to 50 events for system alert include:

* Device Disconnection Detected
* Device restarted
* RS-485 disconnected
* Tamper on
* Supervised Input (Short)
* Supervised Input (Open)
* AC Power Failure
* Forced door opened
* Held door opened
* Forced door open alarmed
* Held door open alarmed
* Enable all floor relays
* Access denied (Exceeded threshold temp.)
* Access denied (Temp. not measured correctly)
* Access denied (Mask not detected)
* Access granted (Soft temp. violation on check only)
* Access granted (Soft mask violation on check only)
* Access granted (Soft temp. and mask violation on check only)
* Access denied (Exceeded threshold temp. on check only)
* Access denied (Temp. not measured correctly on check only)
* Access denied (Mask not detected on check only)
* Abnormal temp. detected (Exceeded Threshold temp.)
* Abnormal temp. detected (Temp. not measured correctly)
* Mask not detected
* Anti-passback zone alarm detected
* Fire alarm zone alarm detected
* Scheduled lock zone alarm detected
* Occupancy Full Detected
* Occupancy Availability Recovered
* Exit Occurred While Occupancy Count Zero
* Occupancy Count Alert 1 Detected
* Occupancy Count Alert 2 Detected
* Intrusion alarm detected
* Interlock door open denied alarm
* Interlock door open denied alarm (Occupied)
* Occupancy Limit Violation (Count Full)
* Muster zone alarm detected
* 1:1 authentication failed
* 1:1 duress authentication succeeded
* 1:N authentication failed
* 1:N duress authentication succeeded
* Access denied (Invalid access group)
* Access denied (Disabled user)
* Access denied (Invalid period)
* Access denied (Blacklist)
* Access denied (Hard anti-passback)
* Access denied (Forced lock schedule)
* Access denied (Soft anti-passback)
* Fake Fingerprint Detected
* Access Denied (Anti-tailgating)

1. Audit Trail
2. Provide the 2 pre-defined filters
3. Last 1 month
4. Last 3 months
5. Support the user to create a filter using each field item that includes:
6. Datetime
7. User
8. Operator Level
9. IP
10. Category
11. Target
12. Action
13. Modification
14. Security
15. Active Directory
16. Support the synchronizing user data stored in Microsoft Windows Active Directory to BioStar 2.
17. Mobile Access
18. Email Setting
19. Backup & Restore

END OF SECTION

# PART 3 - EXECUTION

1. INSTALLER
2. Contractor personnel shall comply with all applicable state and local licensing requirements.
3. Installer and technician requirements
4. Shall be experienced and qualified to accomplish all work promptly.
5. PREPARATION
6. IP addressing shall be coordinated with the Owner’s responsible IT personnel.
7. INSTALLATION
8. Control signal, communications, and data transmission line grounding shall be installed as necessary to preclude ground loops, noise, and surges from adversely affecting system operation.
9. Carefully follow the instructions in the manufacturers’ installation manual to ensure all steps have been taken to provide a reliable, easy-to-operate system.
10. EXAMINATION
11. All network connections shall be tested for proper levels of performance.

END OF SECTION